

Online Safety Policy

Reconnect Learning · Version 2.0 · Approved September 2026 · Review September 2027

POLICY OWNER: ELLEN KERR – MANAGING DIRECTOR & DSL



Statement of Intent

Reconnect Learning recognises that technology plays a vital and ever-expanding role in education, communication and learning. We are committed to ensuring that all learners, staff, tutors, volunteers, contractors and visitors can access technology safely, responsibly and with confidence.

i Online Safety is a safeguarding responsibility. Online harms are treated with the same seriousness as offline safeguarding concerns. Reconnect Learning adopts a child-centred, trauma-informed and proportionate approach to online safety. Professional curiosity is expected of all staff. Effective online safety relies upon partnership working with families, schools, commissioning local authorities and safeguarding agencies.

This policy applies to all use of technology by learners, staff, tutors, volunteers and contractors in connection with Reconnect Learning — whether on organisation-provided or personal devices, on-site, remotely or during online tuition sessions.

This policy is informed by the following legislation and guidance:

Statutory Guidance & Primary Legislation

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children 2026
- Online Safety Act 2023
- Children Act 1989
- Children Act 2004
- Education Act 2002

Supporting Frameworks

- Counter-Terrorism and Security Act 2015
- Equality Act 2010
- Human Rights Act 1998
- Data Protection Act 2018 & UK GDPR
- Current Ofsted inspection framework and guidance

Legislative Framework

Reconnect Learning's Online Safety Policy is grounded in a comprehensive legislative and statutory framework. All staff are expected to be familiar with the key legislation and guidance that informs this policy.

Statutory Guidance

Keeping Children Safe in Education (KCSIE) 2026

Working Together to Safeguard Children 2026

Primary Legislation

Online Safety Act 2023

Children Act 1989

Children Act 2004

Education Act 2002

Counter-Terrorism and Security Act 2015

Equality Act 2010

Human Rights Act 1998

Data Protection Act 2018

UK General Data Protection Regulation (UK GDPR)

Supporting Frameworks

- Current Ofsted inspection framework and guidance
- UKCIS: Sharing Nudes and Semi-Nudes — Advice for Education Settings (current edition)
- Internet Watch Foundation (IWF) Guidance
- Samaritans Media Guidelines
- ICO Guidance on Data Protection in Education
- CEOP (Child Exploitation and Online Protection) Guidance
- UK Council for Internet Safety (UKCIS) Frameworks
- DfE Filtering and Monitoring Standards (current edition)



This policy should be read alongside the Reconnect Learning Safeguarding and Child Protection Policy, which is the organisation's overarching safeguarding policy. All staff are required to read and comply with both policies.



Scope

This policy applies to all individuals who interact with Reconnect Learning systems, services and online environments — whether on-site, remotely or during online tuition sessions.

People

- Learners
- Staff & Tutors
- Associate Tutors
- Volunteers
- Contractors
- Agency Staff
- Directors
- Visitors
- Commissioning Local Authority Representatives

Activities Covered

- Online tuition and remote learning
- Use of organisation-provided devices and personal devices used for work or learning purposes
- Internet and network access
- Social media and digital communication
- Use of Artificial Intelligence (AI) tools
- Email and messaging platforms
- Video conferencing and virtual classrooms
- Online safeguarding concerns and reporting

Settings Covered

- Organisation premises
- Remote and home working
- Online learning environments
- Personal devices used for work purposes
- Any setting in which Reconnect Learning services are delivered, including learners' homes and community venues

Definition of Online Safety

Reconnect Learning recognises the **four key areas of online risk** identified within Keeping Children Safe in Education (KCSIE) 2026. Each area presents distinct challenges that must be understood, addressed and responded to with professional curiosity and a child-centred approach. Reconnect Learning also recognises the growing risk posed by artificial intelligence, including deepfakes, synthetic media and AI-generated harmful content, which may feature across all four risk categories.



CONTENT: harmful, extremist, violent, sexual content, misinformation.



CONTACT: grooming, exploitation, radicalisation, predators.



CONDUCT: cyberbullying, harassment, online abuse.



COMMERCE: fraud, scams, gambling, unauthorized purchases.

Content Risks

Exposure to harmful or inappropriate material online poses significant risks to children and young people. Reconnect Learning takes all reasonable steps to prevent access to such content and ensures that staff are equipped to recognise and respond to content-related concerns.

Extremist & Violent Content

Material promoting extremist ideologies, terrorism, or graphic violence — including content designed to radicalise, incite hatred or traumatisate young people. Staff must be alert to signs that a learner has been exposed to such material.

Sexual Content

Inappropriate sexual material that is harmful or illegal, including child sexual abuse material (CSAM), age-inappropriate content and AI-generated sexual imagery. Any suspected CSAM must be reported to the DSL immediately and to the Internet Watch Foundation (IWF).

Misinformation & Deepfakes

False or misleading information — including AI-generated misinformation, synthetic media, deepfakes and manipulated content — that may cause harm, distress or confusion to learners or undermine their trust in legitimate sources.

Self-Harm & Suicide Content

Content that promotes, glorifies or provides instruction on self-harm, suicide, eating disorders or harmful online challenges. Reconnect Learning follows safe messaging guidelines and the Samaritans Media Guidelines when responding to such concerns.

AI-Generated Harmful Content

Content produced using artificial intelligence tools — including AI-generated images, synthetic audio, deepfakes and algorithmically recommended harmful material — that may be used to exploit, manipulate or harm children and young people.

Contact, Conduct & Commerce Risks

KCSIE 2026 identifies contact, conduct and commerce as three of the four key risk categories. Reconnect Learning ensures that all staff can recognise and respond to risks in each area, applying professional curiosity and a child-centred approach.

Contact Risks

Risks arising from interaction with others online:

- Grooming by adults or peers
- Child sexual exploitation (CSE)
- Child criminal exploitation (CCE)
- Radicalisation and extremism
- Online predators
- Unwanted or inappropriate contact
- AI-assisted grooming

Conduct Risks

Risks resulting from online behaviour:

- Cyberbullying and online harassment
- Sharing harmful or intimate images
- Peer-on-peer abuse
- Harmful sexual behaviour (HSB)
- Sexting and youth-produced sexual imagery
- Online abuse and coercive control
- Impersonation and identity fraud

Commerce Risks

Risks involving financial exploitation:

- Online fraud and scams
- Gambling and gaming exploitation
- Financial grooming and exploitation
- Sextortion (financial)
- Unauthorised purchases
- Subscription traps
- Cryptocurrency scams targeting young people

Roles and Responsibilities

Clear accountability is essential to effective online safety. Reconnect Learning assigns specific responsibilities to all stakeholders in line with KCSIE 2026 and Working Together to Safeguard Children 2026.

01	02
Managing Director / DSL – Ellen Kerr Has overall responsibility for online safety policy and practice. Ensures the policy is implemented, reviewed and updated annually. Receives and acts upon all online safety concerns. Liaises with schools, commissioning Local Authorities and external safeguarding agencies. Ensures all staff receive appropriate and up-to-date training. Maintains oversight of filtering and monitoring arrangements, recognising that where tuition is delivered in learners' homes or community settings, direct control of devices and networks may rest with families or commissioning partners. Leads the organisation's response to online safety incidents.	Staff and Tutors Must read, understand and comply with this policy at all times. Maintain professional boundaries in all online interactions. Use only approved platforms and communication methods. Report all online safety concerns immediately to the DSL — never investigate independently. Model safe, responsible and professional online behaviour. Complete all required online safety training. Apply professional curiosity when working with learners.
03	04
Learners Are supported to use technology safely, responsibly and confidently. Are encouraged to report concerns to their tutor or the DSL without fear of blame. Are expected to respect others online and protect their own personal information. Receive age-appropriate online safety education as part of their learning programme.	Parents and Carers Reconnect Learning recognises the vital role parents and carers play in online safety. Where appropriate, online safety guidance will be shared, support services signposted and collaborative working encouraged. Parents and carers are encouraged to report any online safety concerns relating to their child directly to the DSL. Where tuition is delivered in the home, parents and carers play a particularly important role in supporting safe online practice and are encouraged to engage with the guidance provided by Reconnect Learning.
05	
Commissioning Local Authorities Reconnect Learning will cooperate fully with commissioning local authorities in relation to online safety concerns, safeguarding referrals and information sharing. All relevant concerns will be reported in line with local safeguarding procedures and the organisation's statutory duties.	

Online Learning and Remote Tuition

Reconnect Learning provides online tuition and remote learning where appropriate. All sessions must be conducted professionally, safely and in accordance with this policy and the organisation's safeguarding responsibilities. Online tuition carries the same safeguarding obligations as face-to-face provision.

Approved Platforms

- Microsoft Teams
- Zoom (where approved)
- Google Meet (where approved)
- Approved Virtual Learning Environments (VLEs)
- Organisation-approved communication tools only
- No personal or unapproved platforms permitted

Approved platforms are reviewed periodically by the Managing Director/DSL to ensure they continue to meet safeguarding, privacy and security requirements.

Session Requirements

- Use organisation-provided professional accounts
- Enable waiting rooms before admitting learners
- Use password-protected meeting links
- Use a professional, neutral background
- Dress appropriately and professionally
- Ensure sessions are conducted in a visible, professional setting
- Follow all safeguarding procedures throughout

One-to-One Tuition Safeguards

- One-to-one sessions must be pre-authorised
- Parents/carers must be informed of session arrangements
- Sessions must not be conducted in private or hidden settings
- A second adult should be contactable throughout the session where possible, in line with safer working practice.
- Any concerns arising during a session must be reported to the DSL immediately
- Individual learner risk assessments may identify additional safeguarding measures for particular learners or online tuition arrangements.

Managing Online Behaviour

- Tutors must end sessions immediately if a learner behaves inappropriately
- Any safeguarding concern arising during a session must be reported to the DSL without delay
- Session interruptions or technical failures must be documented
- Tutors must not attempt to manage serious concerns alone — escalate to the DSL



Staff Must Not: Use personal social media accounts, email addresses or messaging services for tuition or learner communication · Share personal contact details with learners or families · Record sessions without prior written authorisation from the DSL and the informed consent of parents/carers · Conduct sessions in inappropriate or private settings · Allow unauthorised third parties to observe sessions

Acceptable Use of Technology

Technology must be used safely, responsibly and legally by all users of Reconnect Learning systems and services. Misuse of technology — including personal devices used for work purposes — may result in disciplinary action and, where a safeguarding concern is identified, referral to the DSL.



No Illegal Material

Accessing, downloading, storing or sharing illegal material — including child sexual abuse material (CSAM), extremist content or material that incites hatred — is strictly prohibited and will result in immediate referral to the police.



No Offensive Content

Sharing offensive, harmful, discriminatory or inappropriate content — including AI-generated harmful material, deepfakes or synthetic media — is not permitted under any circumstances.



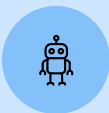
No Cyberbullying

Engaging in cyberbullying, online harassment, trolling or intimidation of any kind is a serious breach of this policy and will be treated as a safeguarding concern.



No Security Bypass

Downloading unauthorised software, circumventing filtering or monitoring systems, or attempting to bypass security measures is strictly forbidden and may constitute a criminal offence.



No Unauthorised AI Use

Using AI tools that have not been approved by the organisation — or using approved AI tools in ways that breach this policy — is prohibited. AI must never be used to process confidential learner information.



Approved Platforms Only

All communication with learners, families and colleagues must take place through organisation-approved platforms only. Personal email addresses, messaging apps and social media accounts must not be used for work communications.



Report Misuse

Any suspected misuse of technology — by staff, learners or others — must be reported to the DSL immediately. Staff must not investigate independently or attempt to resolve concerns without DSL involvement.

Social Media

Professional boundaries must be maintained at all times when using social media. Reconnect Learning requires all staff to uphold the organisation's values and safeguarding responsibilities in all online interactions — whether on personal or professional accounts.

- ☐ Any authorised social media activity on behalf of Reconnect Learning must reflect the organisation's values, professional standards, safeguarding responsibilities and this policy at all times.

Breaches of social media boundaries will be treated as a safeguarding concern and managed in accordance with the Staff Code of Conduct, the Low-Level Concerns Policy and relevant disciplinary procedures. Where a criminal offence may have been committed — including the sharing of intimate images without consent — the matter will be referred to the police without delay.

Staff Must Not

- Accept learner friend or follow requests on personal accounts
- Follow learners on personal social media accounts
- Communicate with learners or families through personal social media
- Share confidential, sensitive or learner-identifiable information online
- Post content that could bring Reconnect Learning into disrepute
- Use personal social media during online tuition sessions
- Post comments about learners, families or colleagues on any online platform

Staff Must

- Use only organisation-approved platforms for professional communication
- Maintain clear professional boundaries in all online interactions
- Report any social media contact from learners or families to the DSL
- Report any safeguarding concerns identified through social media immediately
- Be aware that personal social media activity may be visible to learners and families

Cyberbullying

Reconnect Learning has a **zero-tolerance approach** to cyberbullying in all its forms. All incidents will be taken seriously, recorded and managed in accordance with the Behaviour Policy and Safeguarding and Child Protection Policy.

Cyberbullying may take many forms, all of which are taken seriously by Reconnect Learning. Staff must be alert to signs that a learner is experiencing cyberbullying and respond with professional curiosity and a child-centred approach.



Threatening Messages

Sending threatening, intimidating or abusive messages through any digital channel — including messaging apps, social media, gaming platforms and email.



Harassment & Exclusion

Persistent harassment, deliberate exclusion from online groups or communities, and coordinated online campaigns designed to isolate or humiliate a young person.



Impersonation

Creating fake profiles, impersonating others online, or using AI tools to generate synthetic content designed to cause harm, embarrassment or reputational damage.



Image Sharing

Sharing images or videos of others without consent — including intimate images, humiliating content and AI-generated or deepfake imagery — constitutes image-based abuse and may be a criminal offence.



Online Trolling

Repeated, targeted online abuse designed to provoke distress — including on gaming platforms, social media and online forums. Trolling may escalate to more serious forms of online abuse.



Sextortion

Blackmail involving threats to share intimate images unless demands are met. Sextortion is a serious criminal offence and must be reported to the DSL immediately. The Internet Watch Foundation (IWF) and police should be involved where appropriate.

Signs a Learner May Be Experiencing Cyberbullying

- Withdrawal from online activities or devices
- Visible distress during or after online sessions
- Reluctance to discuss online activity
- Changes in mood or behaviour
- Unexplained avoidance of peers or social situations

Responding to Cyberbullying

- Report immediately to the DSL
- Record the concern accurately and promptly
- Do not advise the learner to delete evidence
- Support the learner in a calm, non-judgmental way
- Follow the Behaviour Policy and Safeguarding and Child Protection Policy
- Where a criminal offence may have been committed, refer to the police

Harmful Sexual Behaviour and Online Abuse

Reconnect Learning recognises the serious risks associated with online sexual harm and abuse, including harmful sexual behaviour (HSB) between children and young people. All concerns are treated with the utmost seriousness and managed in accordance with KCSIE 2026 and the organisation's Safeguarding and Child Protection Policy.

Recognised Risks

- Online sexual harassment and coercion
- Sexualised language and behaviour in online settings
- Peer-on-peer abuse with an online element
- Sharing nudes and semi-nudes (youth-produced sexual imagery)
- Child sexual exploitation (CSE) facilitated online
- Image-based abuse and non-consensual sharing of intimate images
- Sextortion (financial or sexual blackmail)
- AI-generated child sexual abuse material (CSAM)
- Deepfake sexual imagery targeting children or young people
- Online grooming leading to sexual abuse

Response Framework

- Report immediately to the DSL — never investigate independently
- Follow KCSIE 2026 and the Safeguarding and Child Protection Policy
- Record the concern accurately using the learner's own words
- Do not advise the learner to delete evidence
- The DSL will assess and refer to Children's Social Care or police as appropriate
- The Internet Watch Foundation (IWF) should be notified of any CSAM
- Support will be provided to the learner throughout the process

Sharing Nudes and Semi-Nudes

- Managed in accordance with UKCIS: Sharing Nudes and Semi-Nudes — Advice for Education Settings (current edition)
- Treated as a safeguarding concern, not primarily a disciplinary matter
- The DSL leads the response — not the tutor
- Parents/carers informed where appropriate and safe to do so
- Images must not be viewed, downloaded or shared by staff

⊗ Concerns relating to harmful sexual behaviour or online sexual abuse must be reported **immediately** to the DSL. Staff must never investigate independently, view or share images, or attempt to resolve concerns without DSL involvement. Where a learner is at immediate risk of harm, contact emergency services (999) immediately — do not wait to speak to the DSL.

Online Safeguarding Concerns

Staff must be alert to a wide range of online safeguarding concerns and respond promptly, professionally and in accordance with this policy and the Safeguarding and Child Protection Policy. Professional curiosity is essential – staff must never dismiss concerns or wait for certainty before acting – professional curiosity requires active enquiry, not passive observation.



1	2	3
Report Immediately All concerns must be reported to the DSL without delay – the same day the concern arises. Do not wait for certainty. Do not investigate independently.	Record Factually Document concerns accurately and contemporaneously using factual, objective language. Use the learner's own words where a disclosure has been made. Do not edit or interpret.	Follow Procedures Adhere to the Safeguarding and Child Protection Policy and this policy at all times. Where a learner is at immediate risk of harm, contact emergency services (999) immediately – do not wait to speak to the DSL.

Artificial Intelligence (AI)

Reconnect Learning recognises the rapidly growing use of artificial intelligence (AI) technologies in education, professional settings and everyday life. AI may support learning and professional practice where appropriate, but must be used responsibly, ethically and in full compliance with this policy and the organisation's safeguarding responsibilities.

i AI presents both opportunities and risks. Reconnect Learning is committed to ensuring that all staff and learners understand how to use AI safely, critically evaluate AI-generated content, and recognise when AI is being used to cause harm.

AI Must Not Be Used To

Create, generate or share harmful, illegal or inappropriate content	Produce or distribute AI-generated sexual imagery (including deepfakes)
Facilitate grooming, exploitation or abuse	Access, process or share confidential or personal learner information
Circumvent safeguarding, filtering or monitoring arrangements	Facilitate academic dishonesty or plagiarism
Generate or spread misinformation or disinformation	Impersonate individuals or create synthetic identities

Learner Use of AI

- Learners may use AI tools only where explicitly approved by their tutor
- Learners must be taught to critically evaluate AI-generated content
- Learners must not share personal information with AI tools
- Learners must not use AI to produce harmful, offensive or dishonest content
- Digital resilience and critical thinking are embedded in the learning programme

i Staff remain professionally accountable for all safeguarding decisions. AI tools may support professional practice but must never replace professional judgement. All safeguarding decisions must be made by appropriately trained staff, regardless of any AI-generated output. The use of artificial intelligence within Reconnect Learning will be reviewed regularly to ensure it remains safe, lawful, ethical and appropriate for educational use.

Staff Using AI Must

- Verify and critically evaluate all AI-generated information before use
- Protect learner confidentiality and personal data at all times
- Comply with the Data Protection Act 2018 and UK GDPR at all times
- Maintain professional judgement — AI does not replace safeguarding responsibilities
- Report any AI-related safeguarding concerns to the DSL immediately
- Disclose AI use transparently where relevant to learners or families
- Remain alert to AI-assisted grooming, deepfakes and synthetic media

Emerging AI Risks

- AI-generated images and deepfakes used to exploit or manipulate
- Synthetic audio used for impersonation or grooming
- Algorithm-driven recommendations promoting harmful content
- AI-assisted grooming and exploitation
- AI-generated misinformation targeting vulnerable young people
- Generative AI used to produce child sexual abuse material (CSAM)

Filtering and Monitoring

Reconnect Learning will ensure that any devices, networks or online platforms provided directly by the organisation are subject to appropriate filtering and monitoring arrangements, proportionate to identified risks and in line with the requirements of Keeping Children Safe in Education (KCSIE) 2026.



Reconnect Learning recognises that, where tuition is delivered in learners' homes or community settings, direct control of devices and networks rests with families or commissioning partners. In these contexts, Reconnect Learning will work collaboratively with parents/carers, schools and commissioning local authorities to promote safe online practice and respond appropriately to identified online risks.



Website Filtering

Filtering systems restrict access to harmful, inappropriate or illegal online content. Filtering arrangements are proportionate to the age and vulnerability of learners and are reviewed regularly. The DSL and senior leadership maintain oversight of filtering systems and understand how they operate.



Safeguarding Alerts

Automated alerts flag potential safeguarding concerns for immediate review by the DSL. All alerts are treated as potential safeguarding concerns and assessed promptly. Filtering does not replace staff vigilance — it supports it.



Security Monitoring

Ongoing monitoring of network and device activity to identify and respond to security threats, policy breaches and safeguarding concerns. Monitoring is risk-based and proportionate. Staff are aware that monitoring is in place.



Usage Monitoring

Usage patterns are monitored and access restrictions applied where necessary. Monitoring arrangements are reviewed as technology changes and new risks emerge. Records of monitoring activity are maintained by the DSL.



Filtering and monitoring arrangements are reviewed at least annually — and more frequently where new risks are identified. The DSL maintains a record of all filtering and monitoring arrangements and ensures that senior leadership understands and oversees these systems.

Reconnect Learning recognises that filtering and monitoring systems are an important component of safeguarding but are not a substitute for effective staff vigilance, professional curiosity, robust safeguarding procedures and a culture of openness in which learners feel safe to report concerns.

Filtering Principles

- Filtering arrangements are proportionate to the age, vulnerability and identified risks of learners
- Filtering arrangements are reviewed regularly
- Over-blocking is avoided where it restricts legitimate learning
- Under-blocking is addressed promptly when identified
- Filtering supports — but does not replace — staff safeguarding responsibilities

Monitoring Principles

- Monitoring is risk-based and proportionate
- Staff are informed that monitoring is in place
- Monitoring arrangements are reviewed as technology evolves
- All monitoring alerts are assessed promptly by the DSL or a nominated deputy
- Monitoring records are maintained and available for inspection

Personal Devices and Data Protection

Reconnect Learning recognises that staff may use personal devices for work purposes, particularly in remote and home-working contexts. All use of personal devices for work purposes must comply with this policy, the organisation's Data Protection Policy, Acceptable Use Policy and safeguarding responsibilities.

Personal Devices (BYOD)

Where personal devices are used for work purposes (Bring Your Own Device — BYOD), staff must:

- Use strong, unique passwords and enable multi-factor authentication (MFA)
- Enable device encryption and security features
- Keep devices and software up to date
- Never store learner information on unsecured personal devices
- Avoid using public or unsecured Wi-Fi networks for work purposes
- Use a VPN where required and available when working remotely
- Report lost or stolen devices to the DSL and IT lead immediately
- Ensure learner information is stored only on approved, secure platforms
- Log out of all work accounts when not in use

❌ Learner information must **never** be stored on unsecured personal devices. Any loss or theft of a device containing learner data must be reported to the DSL immediately as a potential data breach under the Data Protection Act 2018 and UK GDPR.

Remote Working Expectations

- Use only approved platforms and communication tools
- Ensure your working environment is private and professional during online sessions
- Do not allow family members or others to observe confidential sessions
- Secure all devices when not in use
- Follow the organisation's remote working guidance at all times

Data Protection & Privacy

All users must comply with:

- UK GDPR
- Data Protection Act 2018
- Reconnect Learning Data Protection Policy
- Reconnect Learning Acceptable Use Policy

Personal data must be stored securely, shared only on a need-to-know basis, and protected from unauthorised access at all times. Data breaches — including loss of devices, accidental disclosure or unauthorised access — must be reported to the DSL immediately.

Reporting Device Loss or Data Breaches

- Report immediately to the DSL and IT lead
- Do not attempt to investigate independently
- The DSL will assess, in consultation with the Data Protection Officer or nominated lead, whether a formal data breach report to the Information Commissioner's Office (ICO) is required within 72 hours
- All incidents will be recorded and reviewed
- Remote wipe of lost or stolen devices will be initiated where possible

Reporting Online Safety Concerns

All online safety concerns must be reported **immediately**. Do not delay, investigate independently, or attempt to resolve concerns without involving the DSL.

 If a learner is at immediate risk of harm, contact emergency services (999) immediately. Do not wait to speak to the DSL before calling 999.

01	02
Recognise Identify that an online safety concern may exist. Trust your instincts — you do not need to be certain that harm has occurred. Apply professional curiosity. Signs may include changes in behaviour, distress, disclosure, or concerning online activity.	Record Make a clear, factual, contemporaneous record of the concern. Use the learner's own words where a disclosure has been made. Do not edit, interpret or delay your record. Include date, time, what was said or observed, and who was present.
03	04
Report to the DSL Report your concern immediately to the Designated Safeguarding Lead (DSL): Ellen Kerr – Managing Director. If the DSL is unavailable, report to the Deputy DSL or the most senior member of staff available. Concerns must be reported on the same day they arise — never delayed.	DSL Assessment The DSL will assess the concern, consult with relevant agencies where appropriate, and determine the appropriate course of action. The DSL may seek advice from the Local Authority Designated Officer (LADO), the Multi-Agency Safeguarding Hub (MASH), or other relevant safeguarding partners.
05	
Referral or Support Where appropriate, the DSL will make a referral to Children's Social Care, the police or other relevant agencies. Support will be arranged for the learner and, where appropriate, their family. All actions will be recorded and reviewed.	

Concerns That Must Be Reported

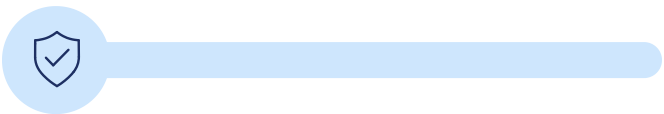
- Grooming or suspected grooming
- Child sexual exploitation (CSE) or child criminal exploitation (CCE)
- Cyberbullying causing significant distress
- Radicalisation or extremist content
- Harmful sexual behaviour online
- Sextortion or sharing of intimate images
- Online abuse or harassment
- AI-assisted exploitation or deepfake abuse
- Any disclosure of online harm or abuse made by a learner, however minor it may appear

Key Principles

- Never investigate independently
- Never promise confidentiality to a learner
- Never wait for certainty before reporting
- Always record concerns accurately and promptly
- Always follow the DSL's guidance
- The decision to refer to external agencies rests with the DSL — not the reporting member of staff
- All concerns are taken seriously, however minor they may appear

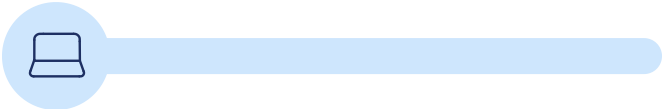
Training Requirements

All staff will receive comprehensive training to ensure they are equipped to fulfil their online safety responsibilities. Training will be refreshed regularly, records of completion maintained, and training needs reviewed annually by the DSL. Training requirements reflect the organisation's delivery model, including online tuition, home tuition and alternative provision.



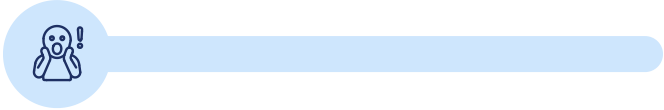
Safeguarding Training

Core safeguarding knowledge and responsibilities for all staff working with children and young people, including recognition of abuse, reporting procedures and the role of the DSL. Refreshed at least annually in line with KCSIE 2026 requirements.



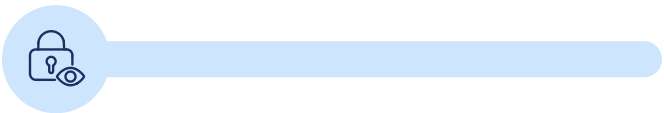
Online Safety Training

Specific training on online risks, safe use of technology, responding to online safeguarding concerns, filtering and monitoring, and emerging online threats including AI risks. Refreshed at least annually and updated as new online risks emerge.



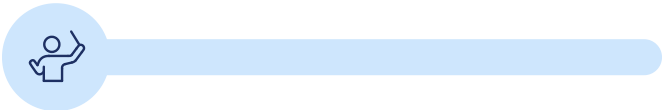
Prevent Duty Training

Training on recognising and responding to radicalisation and extremism in line with the Counter-Terrorism and Security Act 2015 and the Prevent Duty. Includes online radicalisation and extremist content.



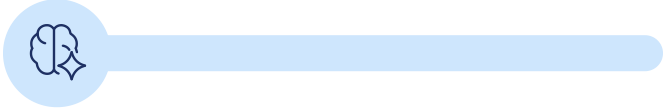
Data Protection Training

Understanding of UK GDPR, Data Protection Act 2018, and Reconnect Learning's data handling responsibilities — including secure use of personal devices, remote working and data breach reporting.



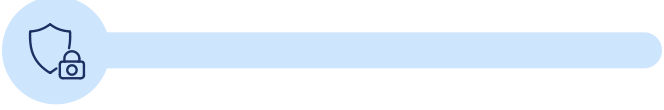
Staff Code of Conduct Training

Ensuring all staff understand professional boundaries, acceptable use of technology, social media expectations and behavioural standards — including online interactions with learners and families.



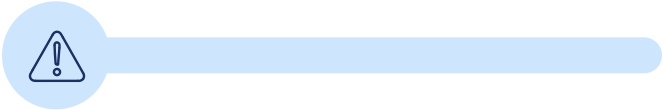
AI Safeguarding Training

Training on the safeguarding risks associated with artificial intelligence — including deepfakes, synthetic media, AI-assisted grooming, AI-generated harmful content and responsible use of AI in education.



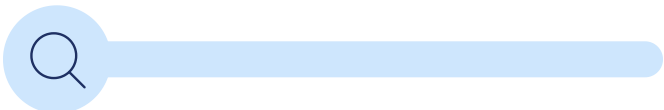
Cyber Security Awareness

Training on cyber security threats, phishing, password security, multi-factor authentication, secure remote working and reporting of cyber incidents.



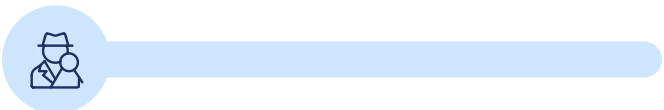
Harmful Sexual Behaviour & Sextortion

Training on recognising and responding to harmful sexual behaviour (HSB) online, sexting, youth-produced sexual imagery, sextortion and online sexual abuse — including referral pathways.



Digital Resilience & Misinformation

Training on supporting learners to develop digital resilience, critical evaluation of online content, recognition of misinformation, deepfakes and algorithm-driven harmful content.



Professional Curiosity

Training on applying professional curiosity in online safety contexts — recognising subtle signs of concern, asking the right questions, and not accepting surface-level explanations where concerns exist, and understanding that online harm may not always be immediately visible.

Monitoring and Review

The Managing Director and DSL will maintain ongoing oversight of online safety arrangements to ensure they remain effective, compliant and responsive to emerging risks. This policy is a living document and will be reviewed annually and without unnecessary delay following changes to legislation, statutory guidance, safeguarding practice, organisational arrangements or learning from safeguarding incidents.



i This policy will be reviewed annually and without unnecessary delay following changes to legislation, statutory guidance, safeguarding practice, organisational arrangements or learning from safeguarding incidents. This policy was approved in September 2026. Next review: September 2027. Policy Owner: **Ellen Kerr – Managing Director & DSL.**

Related Policies & Commitment

This policy should be read alongside the following Reconnect Learning policies. Together, these policies form the organisation's comprehensive safeguarding and compliance framework.

- Safeguarding and Child Protection Policy
- Prevent Duty and Radicalisation Policy
- Staff Code of Conduct
- Safer Recruitment Policy
- Behaviour Policy
- Low-Level Concerns Policy
- Allegations Against Staff Policy
- Whistleblowing Policy
- Data Protection Policy
- Acceptable Use Policy
- Mobile Device Policy (where applicable)

Our Commitment

Reconnect Learning believes that online safety is an essential and non-negotiable part of safeguarding. We are committed to creating a safe digital environment where children and young people can learn, develop and thrive — protected from online harm, abuse and exploitation. Reconnect Learning is committed to fostering a culture of continuous improvement, recognising that online risks evolve rapidly and that safeguarding practice must evolve alongside them to ensure children and young people remain safe. This policy will be reviewed annually and without unnecessary delay following changes to legislation, statutory guidance, safeguarding practice, organisational arrangements or learning from safeguarding incidents.

Approved By: Ellen Kerr – Managing Director & DSL

Version: 2.0

Date Approved: September 2026

Review Date: September 2027